What is claimed is:

1. A system for anonymous biometric authentication comprising:

a biometric acquisition device;

a second biometric of an individual seeking to exercise a privilege, said second biometric image captured by said biometric acquisition device;

a database comprising a plurality of first biometrics relating to said privilege; and

a processor coupled to said biometric acquisition device for receiving said second biometric and coupled to said database for accessing said stored first biometrics, said processor having a comparator for comparing said second biometric to said first biometrics stored in said database, wherein an anonymous biometric authentication of an identity of said individual is based on said comparison of said second captured biometric to said first stored biometric.

2. The system according to claim 1, wherein said privilege is granted based on the result of said anonymous biometric authentication of an identity of said individual.

3. The system according to claim 1, wherein said database further comprises a good database comprising a plurality of first biometrics authorized to exercise said privilege, wherein said processor accesses said stored first biometrics in said good database and said comparator compares said second biometric to said first biometrics stored in said good database, wherein said anonymous biometric authentication of an identity of said individual is based on a positive comparison of said second captured biometric image to one of said first stored biometric images in said good database.

4. The system according to claim 3, wherein said privilege is granted to said individual based on a positive anonymous biometric authentication of said identity of said individual indicated by a match of said second biometric to one of said first biometrics stored in said good database.

5.   The system according to claim 1, wherein said database further comprises a bad database comprising a plurality of first biometrics not authorized to exercise said privilege, wherein said processor accesses said stored first biometrics in said bad database and said comparator compares said second biometric to said first biometrics stored in said bad database, wherein said anonymous biometric authentication of an identity of said individual is based on a positive comparison of said second captured biometric image to one of said first stored biometric images in said bad database.

6.   The system according to claim 5, wherein said privilege is granted to said individual based on a negative anonymous biometric authentication of said identity of said individual indicated by no match of said second biometric to any of said first biometrics stored in said bad database.

7.   The system according to claim 1, further comprising a transaction request that is received by said processor along with said second biometric, wherein said second captured biometric is compared by said processor said first biometrics stored in said database corresponding to said transaction request in order to grant said privilege corresponding to said transaction request.

8.   The system according to claim 1, further comprising a transaction number that is received by said processor along with said second biometric, said transaction number being indicative of a specific transaction of said privilege which is exercised by said individual.

9.   The system according to claim 1, wherein said second captured biometric is compared by said processor to all of said first biometrics stored in said database in order to verify said identity of said individual.

10.   The system according to claim 1, wherein said biometric is an iris of an eye.

11.   The system according to claim 1, wherein said biometric acquisition device is an iris acquisition device for capturing an image of an iris of an eye of said individual.

12.   The system according to claim 1, further comprising a second biometric record, said second biometric record comprising a biometric template extracted from said captured second biometric, a transaction request for said privilege sought to be exercised, and a transaction number, wherein said biometric template portion of said second biometric record binds an identity of said individual to said transaction request and said transaction number.

13.   The system according to claim 1, further comprising a first biometric record, said first biometric record comprising a biometric template extracted from said first biometric and said privilege sought to be exercised, wherein said biometric template portion of said first biometric record binds an identity of said individual to said privilege assigned to said individual.

14.   The system according to claim 1, wherein said privilege comprises one of a single privilege and a set of privileges.

15.   The system according to claim 1, wherein said privilege comprises one or more of: access to a building, access to a secure area, cashing a personal check, using a credit card, performing a financial transaction, and fulfilling a reservation.

16.   The system according to claim 1, further comprising an involuntary revocation system for involuntarily revoking said privilege, said involuntary revocation system comprising a temporary database for storing said second biometric and one or more of a transaction request and a transaction number, a verification authority for verifying whether said individual is authorized to exercise said privilege, a rejection code generated by said verification authority if said individual is not authorized to exercise said privilege, and a processor coupled to said verification authority for receiving said rejection code and coupled to said temporary database for retrieving said corresponding second biometric and one or more

of said transaction request and said transaction number and coupled to a good database for comparing said second biometric to said first biometrics stored in said good database, wherein one of said first biometrics matching said second biometric is removed from said good database based on said comparison.

17. The system according to claim 16, further comprising an involuntary revocation record, said involuntary revocation record comprising said second biometric and said rejection code documenting reasons for said involuntary revocation and said involuntary revocation record being stored in a database.

18. The system according to claim 1, further comprising a voluntary revocation system for voluntarily revoking said privilege, said voluntary revocation system comprising a biometric acquisition device, a transaction request to voluntarily revoke said privilege, a second biometric that is voluntarily submitted by an individual seeking to voluntarily revoke said privilege, a processor for accessing said database containing said plurality of first biometrics, and a comparator for comparing said second voluntarily submitted biometric to all of said first biometrics until a match is found, wherein said matching first biometric is removed from said database.

19. The system according to claim 1, wherein said first biometrics and said second biometrics are encrypted to further protect an identity of said individual.

20. The system according to claim 19, wherein said encryption is accomplished using one of public-key and private-key techniques.

21. The system according to claim 1, further comprising a biometric enrollment system comprising:

a biometric acquisition device;

a first biometric of an individual seeking to be enrolled, said first biometric captured by said biometric acquisition device;

one or more credentials indicative of an identity of said individual;

an enrollment authority for verifying an identity of said individual seeking enrollment using said one or more credentials; and

a good database for storing said captured first biometric image, wherein said good database stores a plurality of first biometrics of individuals enrolled in said anonymous biometric authentication system and wherein said credentials are not stored in said good database with said first biometric.

22.	A system for anonymous biometric authentication comprising:

a biometric enrollment system comprising:

a biometric acquisition device;

a first biometric of an individual seeking to be enrolled, said first biometric captured by said biometric acquisition device;

one or more credentials indicative of an identity of said individual;

an enrollment authority for verifying an identity of said individual seeking enrollment using said one or more identification documents;

a good database for storing said captured first biometric after said identity of said individual seeking enrollment has been verified, wherein said good database stores a plurality of first biometrics of individuals enrolled in said anonymous biometric authentication system and wherein said credentials are not stored in said good database with said first biometric;

a biometric authentication system comprising:

a biometric acquisition device;

a second biometric of an individual seeking to exercise a privilege, said second biometric captured by said biometric acquisition device; and

a processor coupled to said biometric acquisition device for receiving said second biometric and coupled to said good database for accessing said stored first biometrics, said processor comparing said second biometric to said first biometrics stored in said database;

wherein an anonymous authentication of said individual is based on said comparison of said second captured biometric to said first stored biometrics and wherein said

privilege is granted based on the result of said anonymous biometric authentication of an identity of said individual.

23. A system for anonymous biometric authentication of an individual for granting of one or more privileges comprising:

a first biometric indicative of an identity of an individual;

one or more credentials indicative of said identity of said individual;

a privilege sought to be exercised by said individual;

a first memory for storing said first biometric of said individual once said identity of said individual has been verified using said credentials, said first memory comprising a plurality of first biometrics for all individuals authorized to exercise said privilege;

a second memory for storing a second biometric obtained by a biometric acquisition device from an individual seeking to exercise said privilege; and

a comparator for comparing said second biometric of said second memory with said plurality of first biometrics of said first memory for anonymous biometric authentication of said individuals authorized to exercise said privilege.

24. The system according to claim 23, further comprising an authentication code generated by said anonymous biometric authentication system granting said privilege based on a positive comparison of said second biometric of said second memory with said first stored biometric of said first memory, wherein said individual associated with said second biometric may exercise said privilege.

25. The system according to claim 23, wherein said biometric comprises an iris of an eye and said biometric acquisition device comprises a camera.

26. The system according to claim 23, wherein said comparator comprises a processor responsive to an output of said biometric acquisition device for comparing said biometric of said second memory with said all of said stored biometrics of said first memory.

27. The system according to claim 23, wherein

said first memory stores at least one template of at least one image of at least one iris of an eye of said individual indicative of said identity of said individual that has been assigned one or more privileges;

said second memory stores a template of an iris image obtained by an iris acquisition device from an iris of an eye of an individual seeking to exercise said one or more privileges; and

said comparator compares said template of said iris image of said second memory with said stored template of said first memory for anonymous biometric authentication of said individual, and wherein no personal identifying information is stored in either of said first memory and said second memory.

28. A method of anonymous biometric authentication of an individual for granting one or more privileges comprising the steps of:

submitting a transaction request indicative of a privilege that is sought to be exercised;

capturing a biometric of an individual;

storing said captured biometric in a memory;

comparing said captured biometric to a plurality of enrolled biometrics stored in a database corresponding to said privilege that is being sought to be exercised;

anonymously authenticating an identity of said individual based on said step of comparing said captured biometric to said stored biometrics in said database; and

granting said privilege based on said step of anonymously authenticating said individual.

29. The method according to claim 28, further comprising generating an authorization code based on said step of anonymously authenticating said individual.

30. The method according to claim 28, further comprising generating an approval authorization code if one of said stored biometrics matches said captured biometric.

31.   The method according to claim 28, further comprising generating one of a rejection authorization code and no authorization code if one of said stored biometrics does not match said captured biometric.

32.   The method according to claim 28, further comprising the step of involuntarily revoking said privileges, wherein said step of involuntarily revoking said privileges further comprises the steps of:

saving said transaction request and said second biometric in a temporary transaction database;

transmitting said transaction request and said second biometric to a verification authority;

verifying said individual submitting said second biometric has been assigned said privilege sought to be exercised;

transmitting an authorization code to said temporary transaction database and finding said transaction request and said second biometric in said temporary transaction database;

searching said good database to find a matching biometric corresponding to said second biometric; and

removing said corresponding first biometric from said good biometric database based on said step of verifying.

33.   The method according to claim 28, further comprising the step of voluntarily revoking said privileges, wherein said step of voluntarily revoking said privileges further comprises the steps of:

receiving a second biometric from an individual seeking to have a privilege voluntarily revoked;

searching said good database to find a matching first biometric; and

removing said first biometric based on said matching.

34.   The method according to claim 28, wherein said step of capturing a biometric of an individual further comprises capturing an iris image of an eye as said biometric of said individual.